Checking IOP Memory Accesses on the DTL-T10000

To: All licensees

2000/02/01
SCE Software Development Division

The following is a description of how accesses to IOP memory above 2 Mbytes can be checked on the DTL-T10000.

If a program does not work properly on the DTL-H10000 debugging station, checking for such accesses can be useful in debugging.

* Procedure

1) Program the EE so that the "mem2MB.irx" IOP module is run, followed immediately by a reboot of the IOP.

Use a break instruction to stop the program before title-specific IOP modules are run. (If proper timing can be determined, the break command can be issued from dsedb.)

```
(Example)
#include <eekernel.h>
#include <eeregs.h>
#include <sifdev.h>
#include <stdio.h>
#include <libcdvd.h>

int main()
{
  sceSifInitRpc(0);
  /* Wait for DiskReady */
  sceCdInit(SCECdINIT);

  /* run mem2MB */
  while ( sceSifLoadModule("host0:mem2MB.irx",0,NULL) < 0);

  /* Replace IOP reboot default module */
  while ( !sceSifRebootIop("cdrom0:\\IOPRP14.IMG;1") );
  while( !sceSifSyncIop() );
  /* reinitialize */
  sceSifInitRpc(0);
  sceCdInit(SCECdINIT);
  sceFsReset();
  /* run non-default modules */
  while (sceSifLoadModule("cdrom0:\\SIO2MAN.IRX;1",0,NULL) < 0);
  while (sceSifLoadModule("cdrom0:\\PADMAN.IRX;1",0,NULL) < 0);
    :
  /* stop program */
  asm ("break");
    :
  /* run title-specific modules */
  while (sceSifLoadModule("cdrom0:\\MAIN.IRX;1", 0, NULL) < 0);
    :
    :
}
```

2) Run dsedb and dsidb. Run the EE program from dsedb.
Check mem2MB messages from dsidb.

```
(Example: from dsedb)
dsedb S> run main.elf
Loading program (address=0x00200000 size=0x0000c6c6) ...
       :
*** Resetted
*** No Connect
*** Resetted
       :
*** Unexpected reply - type=BREAKR result=EXCEPTION
*** Target program stopped. Check the location by dr command.
dsedb S>
```

```
(Example: from dsidb)
       :
loadmodule: fname host0:mem2MB.irx args 0 arg
mem2MBpre: Memory limit was changed 8MB to 2MB
loadmodule: id 31, ret 1
Get Reboot Request From EE
*** Resetted
Update rebooting..
       :
```

3) When the EE program stops, use the hardware break feature on dsidb to set a breakpoint if access is attempted in the 2M - 4M area.

```
(Example: from dsidb)
dsidb R> hbp dauk:00200000,50200000
dsidb R> hbp pcuk:00200000,50200000
```

4) Continue EE program.

```
(Example: from dsedb)
dsedb S> sr $epc $epc+4
dsedb S> cont
```

5) If access to the 2M - 4M area is attempted during execution of IOP modules, the following will be output from dsidb and a breakpoint will occur.

```
(Example: from dsidb)
*** Unexpected reply - type=BREAKR code=ff result=DEBUG_EXCEPTION
*** Target program stopped. Check the location by dr command.
dsidb S>
dsidb S> dr
 at=00020024  v0-1=00200000,11111111  a0-3=00000001,...
       :
 $cr=0x10000024 [ CE1 Breakpoint ]
 $sr=0x00000404 [ IM0 IEp ]
  0x00066e9c: 0x3c031111  lui     $v1,0x1111  # 0x11111111
  0x00066ea0: 0x34631111  ori     $v1,$v1,0x1111
```

```
->0x00066ea4: 0xac430000  sw      $v1,0($v0)
       :
```

6) Then set up breakpoints as described above to catch accesses in the 4M - 8M area.

```
(Example: from dsidb)
dsidb R> hbp dauk:00400000,50400000
dsidb R> hbp pcuk:00400000,50400000
```

[Version history]
99/01/29 Registered
99/02/01 Modified